REMARKS

Claims 1-2, and 4-47 are presented for examination. Claims 1, 2, 4, 5, 13, and 21-24 have previously been amended and claim 3 has previously been canceled as set forth in the amendment filed with the Request for Continued Examination. This preliminary amendment adds new claims 25-47 for examination.

New claim 25 is essentially claim 1 in which the limitation of diffusing the confused document by performing an EXOR operation has been removed. Applicants respectfully submit that claim 25 is allowable over the references previously cited and applied by the Examiner because the method includes confusing characters belonging to an electronic input document through an invertible scrambler to obtain a confused document having a plurality of confused characters in which each string of characters to be encrypted is added to strings of confused characters obtained by multiplying strings of previously confused characters by respective multiplication constants. Nowhere do Dachselt et al. or Bianco, both of which are of record, taken alone or in any combination thereof, teach the combination recited in claim 1 for protecting the contents of an electronic document that has a plurality of strings of characters to be encrypted. More particularly, neither of these references teach or suggest adding each string of characters to be encrypted to strings of confused characters that have been obtained by multiplying strings of previously confused characters by respective multiplication constants. In other words, in claim 1, the method uses a fed-back chaotic system applied to a previously confused document. Such a method is not taught or suggested in either of the references cited by the Examiner, taken alone or in any combination therewith. Applicants respectfully submit that new claim 25 is clearly allowable.

Dependent claims 26-35 are allowable for the features recited therein as well as for the reasons why claim 25 is allowable.

Independent claim 36 is directed to a device for protecting the contents of an electronic document having a plurality of strings of characters to be encrypted. The device includes a confusion block for confusing an electronic input document, the confusion block comprising an invertible scrambler that supplies a confused document, the confused document comprising a plurality of confused characters, and the confusing block adapted to add each string of characters to be encrypted to strings of characters obtained by multiplying the strings of

previously confused characters by respective multiplication constants and a diffusion block cascade-connected to the confusion block, the diffusion block comprising mixing means for mixing the confused document with chaotic characters, which supply an encrypted document. Neither Dachselt et al. nor Bianco, taken alone or in any combination thereof, teach or suggest a confusing block adapted to add each string of characters to be encrypted to strings of confused characters that are obtained by multiplying strings of previously confused characters by respective multiplication constants. Moreover, neither of these references teach or suggest the foregoing in combination with a diffusion block cascade-connected to the confusion block, the diffusion block having mixing means for mixing the confused document with chaotic characters to supply an encrypted document. Applicants respectfully submit that independent claim 36 is clearly allowable over the references cited and applied by the Examiner.

Dependent claims 37-43 are allowable for the features recited therein as well as for the reasons why claim 36 is allowable.

New independent claim 44 is directed to a method of protecting the contents of an electronic document in which acquired encryption keys having an initial chaotic value are used to generate confused character strings by calculation using the input character strings, the encryption keys, and previously confused character strings to obtain a confused word. Claim 44 further recites calculating a current chaotic value from the initial chaotic value, and calculating an encrypted word by performing a mixing operation on the confused word and the current chaotic value to obtain an encrypted word. Applicants respectfully submit that claim 44 is clearly allowable over Dachselt et al. and Bianco for the reasons discussed above with respect to claims 25 and 36, in that neither of these references teach or suggest using previously confused character strings to obtain a confused word. Dependent claim 45 is also allowable for the features recited therein as well as for the reasons why claim 44 is allowable.

New independent claim 46 is directed to a method for protecting the contents of an electronic document that includes calculating a confused character string initially using input character strings, encryption keys, and the contents of shift registers, and repeating the acquisition of the input character string, calculating the confused character string, and feeding the confused character string to shift registers a predetermined number of times to obtain a plurality of confused character strings. Claim 46 further recites calculating a subsequent chaotic

value using the contents of the chaotic value register and performing a mixing operation on the subsequent chaotic value and the plurality of confused character strings to obtain an encrypted word. Claim 47, which depends from claim 46, recites decrypting the encrypted word by adding the encrypted word to a chaotic value identical to the chaotic value and subtracted from a previously decrypted word using an unscrambler element having a structure similar to that of a scrambler that generated the confused word, and further using identical encryption keys.

Applicants submit that claim 46 is clearly allowable over the references cited and applied by the Examiner because neither of these references teach or suggest using a stored previously confused character string in shift registers a predetermined number of times to obtain a plurality of confused character strings, along with the other steps recited therein.

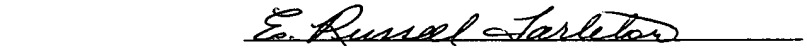
In view of the foregoing, Applicants respectfully submit that all of the claims are now clearly in condition for allowance. In the event the Examiner finds minor informalities that can be resolved by telephone conference, the Examiner is urged to contact Applicants' undersigned representative by telephone at (206) 622-4900 in order to expeditiously resolve prosecution of this application. Consequently, early and favorable action allowing these claims and passing this case to issuance is respectfully solicited.

The Director is authorized to charge any additional fees due by way of this Amendment, or credit any overpayment, to our Deposit Account No. 19-1090.

All of the claims remaining in the application are now clearly allowable. Favorable consideration and a Notice of Allowance are earnestly solicited.

Respectfully submitted,

SEED Intellectual Property Law Group PLLC



E. Russell Tarleton
Registration No. 31,800

ERT:jk
701 Fifth Avenue, Suite 6300
Seattle, Washington 98104-7092
Phone: (206) 622-4900
Fax: (206) 682-6031

785813_1.DOC